



Policy Brief on
**Technology-Facilitated Gender
Based Violence (TFGBV) in Kenya**
June 2026

STATEMENT OF PRINCIPLE: RIGHTS-BASED, FEMINIST, AND CONSTITUTIONALLY GROUNDED APPROACH.

This policy brief has been developed pursuant to a gap analysis that was undertaken in alignment with the core values of CRAWN Trust, including the advancement of women's rights, feminist legal analysis, access to justice, and the protection of democratic space, as well as the mission of the African Women's Development Fund to support rights-based, women-led initiatives that challenge structural inequality and systemic violence. It is grounded in the Constitution of Kenya (2010) and is informed by a commitment to gender equality, human dignity, and accountability in both physical and digital environments.

The policy brief and the gap analysis it flows from explicitly upholds the right to freedom of expression guaranteed under Article 33 of the 2010 Kenyan Constitution, recognizing its centrality to democratic participation, feminist organizing, and civic engagement. At the same time, it affirms that constitutional protection does not extend to conduct that propagates violence, incites harm, or exploits digital spaces to intimidate, harass, or silence women and girls. Consistent with Article 28, which guarantees the inherent dignity of every person, and Article 27, which affirms equality and freedom from discrimination, this gap analysis recognises Technology-Facilitated Gender-Based Violence (TFGBV) as a direct threat to women's dignity, safety, and equal participation in public life.

In line with Article 48, which guarantees access to justice, and Article 21, which places an obligation on the State to respect, protect, promote, and fulfil rights and fundamental freedoms, this gap analysis seeks to strengthen legal and institutional responses to technology-facilitated gender-based violence through evidence-based, survivor-centred, and gender-responsive recommendations. It does not seek to gag, chill, or constrain lawful expression, legitimate dissent, or civic participation. Rather, it is premised on a clear and principled distinction between constitutionally protected speech and conduct that causes real and demonstrable harm, including abuse, harassment, intimidation, and other forms of digital violence disproportionately affecting women and girls across all demographics.

Any recommendations emerging from this policy brief are guided by the principles of proportionality, necessity, and legality, ensuring that proposed enforcement and policy measures are rights-respecting and narrowly tailored to prevent harm and secure accountability without enabling censorship or misuse. This framing reflects CRAWN Trust's feminist commitment to transformative justice, the African Women's Development Fund's emphasis on systemic change and women's agency, and Kenya's constitutional promise of dignity, equality, and justice for all.

Daisy Amdany

Executive Director - CRAWN Trust

EXECUTIVE SUMMARY

Kenya stands at a critical crossroads in its digital transformation. As the pioneer of global innovations such as M-Pesa and Ushahidi, technologies that fundamentally redefined financial inclusion and democratic accountability, the country boasts an extraordinary mobile penetration rate of %149.4 and a mobile money penetration rate of %91. Yet, this rapid technological advancement has outpaced protective guardrails. The very digital ecosystem that establishes Kenya as a continental leader has simultaneously expanded the surface for systemic abuse, forcing women and girls to bear a disproportionate, severe, and rapidly escalating burden of technology-facilitated harm.

Approximately %95 of aggressive online behaviour and disparaging digital imagery is directed at women. Up to %60 of women leaders, journalists, activists and students have already pulled back from digital spaces or left them entirely, to protect themselves from harassment, threats and reputational attacks. This is referred to as radio silencing, and it is not merely a personal tragedy, rather it is a structural threat to Kenya's democracy, its leadership pipeline and its knowledge economy. In 2024 alone, Kenya recorded 579 femicide cases, many of them preceded by digital threats and stalking. Thus, the connection between technology-facilitated violence and physical harm is no longer a matter of debate.

This policy brief emanates from a gap analysis commissioned by CRAWN Trust with support from AWDF, and grounded in Kenya's Constitution, domestic law, and the full spectrum of regional and international human rights standards **maps nine interconnected failures in how Kenya currently responds to technology-facilitated gender-based violence (TFGBV).**

The first and most foundational failure is legislative. Kenya has no standalone, gender-responsive TFGBV law. There is no statutory definition of TFGBV as a distinct category of harm. There are no legal provisions covering AI-generated deepfakes, voice cloning, synthetic intimate imagery or cryptocurrency-enabled sextortion. This gap deepened in October 2025 when the High Court suspended key cyber harassment provisions of the Computer Misuse and Cybercrimes Act, finding the enhanced penalties overbroad. The result is an enforcement vacuum that benefits perpetrators directly.

The second failure is evidentiary. The DCI's National Digital Forensic Laboratory lacks the tools, trained personnel, and protocols to collect and preserve digital evidence to prosecution standards. Survivors routinely wait more than a year for their devices to be returned, a delay that compounds trauma and pushes many into economic precarity.

The third failure is institutional fragmentation. A survivor of AI-generated intimate image abuse may currently be required to navigate the DCI, the Office of the Data Protection Commissioner, Policare,

the ODPP and the Judiciary simultaneously, without an integrated referral pathway, a shared case management system, or a single point of contact who knows her name and case.

The fourth failure is the absence of survivor-centred remedies. Even a successful prosecution changes nothing about the harmful content that remains publicly accessible. Kenya currently has no emergency content removal orders, no right to be forgotten, no interim injunctive relief and no statutory compensation for the reputational, psychological, economic and professional harm that TFGBV causes.

The fifth failure is governance of emerging technology. AI-generated deepfakes, nudify applications, voice cloning, and algorithmically amplified misogynistic content all fall outside current legislation. Kenya's National AI Strategy 2030–2025 does not address the gendered dimensions of AI risk at all.

The sixth failure is awareness. %78 of survivors who participated in this study did not know where to report or seek help at the time of the incident. That figure is not an indictment of survivors, rather it is an indictment of the system.

Three further dimensions complete the picture. Children are already being harmed. The rollout of the Competency Based Curriculum (CBC) has brought AI-driven educational tools into classrooms without adequate parental awareness of data practices, and the Artificial Intelligence Bill 2026 contains no child-specific protections. **Women with disabilities, elderly women and rural women face layered vulnerabilities that a one-size-fits-all framework cannot reach.** And the supply side of TFGBV, **the transnational manosphere ecosystem and platform monetisation models that algorithmically reward harassment, demands regulatory responses** that address commercial incentives, not just individual incidents.

The gap analysis reviewed fifteen domestic legal instruments and fourteen regional and international frameworks, identifying specific gaps and required amendments across all of them. It also assessed the Artificial Intelligence Bill 2026 currently before the Senate, concluding that while it represents a genuine starting point, it requires significant amendment to deliver gender-responsive regulation and to protect Kenyan children from harms that are already occurring on their devices and in their classrooms.

Pursuant to the gap analysis this policy brief has recommendations that span nine thematic areas. At their core the recommendations include; enact a standalone TFGBV Act informed by the UN Women Model Framework. Urgently redraft the suspended CMCA provisions in constitutionally compliant terms. Amend the Data Protection Act, Sexual Offences Act, Protection Against Domestic Violence Act, Kenya Information and Communications Act, Employment Act, Children Act and the National Gender and Equality Commission Act to address TFGBV. Establish a gazetted national TFGBV coordination framework. Build digital forensic capacity with post-quantum cryptographic resilience as a baseline design requirement and not an afterthought, because the quantum computing threat to digital evidence integrity is not a future concern, rather it is already relevant to every piece of survivor evidence being preserved today.

Other recommendations entail the need to create specialist prosecution capacity within the ODPP. Establish Urgent Digital Protection Orders with 24-hour platform compliance timelines. Build a survivor support infrastructure that removes financial barriers and integrates psychosocial, legal and economic empowerment services. Invest in a national TFGBV data observatory. Fully operationalise Kenya's accession to the Budapest and Malabo Conventions and ratify ILO Convention 190. And commission a macroeconomic impact assessment, because addressing TFGBV is not a gender equality initiative running in parallel to Kenya's economic development priorities, it is in fact a precondition for those priorities to be achieved.

This policy brief takes cognizance that while girls and women remain disproportionately affected by TFGBV, men and boys are also impacted by digital harms and insecurity. Accordingly, the recommendations contained herein are designed to promote the safety, dignity, and meaningful participation of all Kenyans within the digital sphere, recognizing that the exclusion of any individual from digital spaces undermines Kenya's socio-economic development, democratic resilience, and national security interests.

As the African proverb reminds us, **"A community is only as strong as the safety and dignity of its people."** This reflects the core premise of this policy brief i.e., that protecting all Kenyans from TFGBV and digital harm is not merely a gender issue, but a national imperative tied to social cohesion, economic progress, democratic participation, and collective security.

MUTHEU NYAGAH KHIMULU -

LLM. Cyber Security, Counter Terrorism & Crisis Management

<https://www.linkedin.com/in/mutheu-khimulu-law/>

Lead Consultant, Policy Brief & Gap Analysis on TFGBV in Kenya

May 2026.

Table of Contents

STATEMENT OF PRINCIPLE: RIGHTS-BASED, FEMINIST, AND CONSTITUTIONALLY GROUNDED APPROACH.....	i
EXECUTIVE SUMMARY	ii
CHAPTER 1: THE CRISIS; WHAT IS HAPPENING TO KENYAN WOMEN ONLINE	1
1.1 Survivor Truths And Systemic Realities.....	1
CHAPTER 2: COMPREHENSIVE LEGISLATIVE AUDIT GAPS, JUSTIFICATIONS & REFORM PATHWAYS3	
2.1: DOMESTIC STATUTORY FRAMEWORKS	3
2.2: REGIONAL AND INTERNATIONAL TREATIES & FRAMEWORKS.....	9
CHAPTER 3: THEMATIC ANALYSIS OF SYSTEMIC BOTTLE NECKS AND EMERGING RISKS	10
CHAPTER 4: STRATEGIC ACTION ROADMAP AND RECOMMENDATIONS.....	12
4.1: Priority Area 1 Immediate Legislative Reform Within 6 Months	12
4.2: Priority Area 2 : Institutional Restructuring And Capacity Building 6 – 18 Months	13
4.3: Priority Area 3 : Survivor-Centred Justice, Data And Platform Accountability Within 18 Months – 3 Years	14
4.4: Horizon Threats: Future-Proofing The Response	15



CHAPTER 1: THE CRISIS; WHAT IS HAPPENING TO KENYAN WOMEN ONLINE.

Kenya's digital revolution is real and so is its shadow. The same infrastructure that powers M-Pesa and connects rural communities is being used, every day, to stalk, humiliate, coerce, and silence women. Technology-Facilitated Gender-Based Violence (TFGBV) i.e. any act of gender-based violence committed, assisted, or amplified through digital technologies, is not a new category of harm rather it is misogyny with a faster network and a permanent record.

TFGBV takes many forms including intimate images shared without consent; harassment campaigns that follow women across platforms; AI-generated sexual imagery of real, named women who never agreed to it; partners who weaponize M-Pesa access and shared passwords as tools of control; and coordinated campaigns designed specifically to drive women journalists, activists, and politicians off the internet entirely.

1.1 SURVIVOR TRUTHS AND SYSTEMIC REALITIES

In March 2026, women who had experienced TFGBV completed a confidential questionnaire at the Wangu Kanja Foundation. Three key findings from their responses deserve the full attention of every institution this policy brief addresses:

- 100% changed their digital behaviour by restricting themselves, withdrawing, or going offline entirely.
- 78% did not know where to report or seek help when the harm happened.
- 67% who did report felt dismissed, mocked, or actively disbelieved by the very authorities they turned to for help.

These are not outliers, but the sad truth of the system working exactly as it is currently built to the continued detriment of those it should protect and as stated in some of their words:

"I had to literally restart life again with nothing in another part of the country for my own physical safety, having narrowly escaped community mob justice."

"My device was taken by police for forensic analysis. More than a year later it had not been returned. I could not work. The cost of reporting was too high to bear again so I won't report again or encourage my friends to."

- Survivors, Wangu Kanja Foundation Questionnaire (March 2026)

These women know exactly what they need i.e. the legal follow-through, trauma-informed officers, rapid content removal, and economic support. They have said it clearly. The question before Kenya's policymakers is not whether those needs have been identified. They have been and the pressing question is whether the state will now build the will to meet them.

CHAPTER 2:

COMPREHENSIVE LEGISLATIVE AUDIT

GAPS, JUSTIFICATIONS & REFORM PATHWAYS

This chapter provides a rigorous statutory and institutional audit designed to optimize Kenya's legal architecture against Technology-Facilitated Gender-Based Violence (TFGBV). By consolidating and examining fifteen domestic legislative instruments, financial regulatory frameworks, and regional or international treaties, this section maps the protective infrastructure of the state. Each instrument is analyzed to identify specific statutory blind spots, real-world survivor implications, and the precise legal amendments required to establish an active, comprehensive, and future-proof justice system.

2.1: DOMESTIC STATUTORY FRAMEWORKS

Statute / Instrument	Current Status & Statutory Context	Identified Gaps & Blind spots	Justification & Survivor Implication	Recommended Reforms & Amendments
Constitution of Kenya (2010)	Grounded in Articles 33, 28, 27, 48, and 21.	Lacks explicit recognition of digital rights or technology-facilitated harms as a constitutional issue.	Survivors must rely on a patchwork of implied protections, leading to procedural uncertainty and inconsistent judicial responses.	Develop progressive judicial benches and clear rules of statutory interpretation that explicitly read digital safety, identity protection, and electronic dignity into Articles 27 and 28.
Computer Misuse and Cybercrimes Act (CMCA)	The primary cybercrime statute, amended in 2024 and 2025. Section 37 covers sharing intimate images.	Key cyber-harassment provisions i.e. Sections (1)27(b), (1)27(c), and (2)27 were suspended by the High Court in October 2025 (Reuben Kigame Lichete & KHRC vs. AG) due to overbreadth. It also lacks definitions for AI deepfakes, voice cloning, and crypto-extortion.	The judicial suspension creates an enforcement vacuum, leaving perpetrators insulated from prosecution and survivors without immediate statutory protection.	Urgently redraft the suspended Section 27 provisions with narrow, precise, and constitutionally compliant language. Introduce a dedicated TFGBV chapter defining AI-generated synthetic harm, cryptocurrency-facilitated sextortion, and mandatory platform notification rules.

Statute / Instrument	Current Status & Statutory Context	Identified Gaps & Blind spots	Justification & Survivor Implication	Recommended Reforms & Amendments
Data Protection Act (DPA), 2019	Sections 31–25 regulate data processing; Section 40 grants data erasure rights; empowers the ODPC.	The framework treats the weaponization of personal data (doxing, intimate image distribution) as an administrative compliance breach rather than an urgent personal safety crisis.	Victims face long administrative delays while their leaked data continues to circulate online, causing ongoing psychological, social, and economic harm.	Amend the DPA to categorize TFGBV-related data as “highly sensitive personal data” requiring expedited handling. Introduce statutory emergency content removal orders and a legal “Right to be Forgotten” with 24-hour compliance timelines for platforms.
Sexual Offences Act (SOA), No. 3 of 2006	Establishes criminal offences for rape, defilement, and sexual assault.	Principal offences require physical contact or physical proximity. It does not recognize virtual sexual violence, non-consensual synthetic intimacy, or AI-facilitated sexual exploitation.	Perpetrators who create and distribute hyper-realistic AI deepfake pornography or engage in severe virtual sexual harassment escape liability under this Act because no physical touch occurred.	Amend the SOA to expand definitions of sexual violence to explicitly include technology-mediated, non-physical sexual offences. Establish an AI consent framework clarifying that a person’s digital likeness cannot be used for sexual imagery without voluntary, informed consent.
Penal Code (Cap. 63)	Contains general criminal law provisions, including criminal intimidation and malicious communications	Offences are based on physical-world threats and lack specific provisions for digital harm dynamics like coordinated swarming, online doxing, or automated harassment.	Prosecutors face challenges when trying to fit complex digital harassment campaigns into old, offline statutory definitions, often leading to charges being downgraded or dismissed.	Modernize Cap. 63 by introducing clear statutory definitions for digital tracking, online stalking, and organized digital intimidation. Ensure that criminal intimidation provisions explicitly cover electronic media and digital communication tools.

Statute / Instrument	Current Status & Statutory Context	Identified Gaps & Blind spots	Justification & Survivor Implication	Recommended Reforms & Amendments
Evidence Act (Cap. 80) & Digital Evidence Standards	Rules governing the admissibility of evidence in all judicial proceedings.	Lacks comprehensive, standardized protocols for authenticating dynamic digital evidence, cloud storage data, or AI-generated synthetic alterations.	Digital evidence is frequently thrown out on technicalities, or survivors are forced to surrender their personal mobile devices to law enforcement for up to a year, compounding their trauma.	Amend Cap. 80 to establish clear, standardized rules for the extraction, hashing, preservation, and admissibility of electronic evidence. Mandate non-invasive data mirroring extraction protocols to prevent the prolonged confiscation of survivors' devices.
Kenya Information and Communications Act (KICA)	Regulates electronic communication, infrastructure, and internet service providers (ISPs).	Focuses primarily on infrastructure management. It lacks explicit statutory obligations for ISPs and content providers regarding content hosting, content moderation, or the immediate removal of harmful material.	Intermediaries operate without clear legal responsibility, allowing abusive content to remain online indefinitely while profit models benefit from high viral engagement.	Amend KICA to introduce conditional intermediary liability. Platforms must lose safe-harbor immunity if they fail to remove verified non-consensual intimate imagery (NCII) or synthetic sexual abuse material within 24 hours of notification.
Protection Against Domestic Violence Act (PADVA), 2015	Protects family members from domestic abuse, emotional distress, and stalking.	Its text focuses primarily on physical and economic domestic harms. It does not explicitly recognize digital coercive control, forced password sharing, or the deployment of hidden spy applications/ stalkerware within intimate relationships.	Survivors of domestic abuse suffer severe, continuous tracking and digital isolation that is frequently dismissed by law enforcement as a private domestic disagreement.	Amend PADVA to introduce “digital coercive control” as a specific domestic offence. Expand Protection Orders to include digital restrictions, legally barring abusers from tracking devices, accessing accounts, or sharing private data.

Statute / Instrument	Current Status & Statutory Context	Identified Gaps & Blind spots	Justification & Survivor Implication	Recommended Reforms & Amendments
Victim Protection Act (VPA), 2014	Coordinates victim support services and safeguards victim dignity throughout legal processes.	Completely omits the psychological and social realities of digital trauma. It provides no specialized protocols for handling “Digital Tattoo” victimization i.e. the ongoing trauma caused by permanent online records of abuse.	TFGBV survivors face severe secondary victimization during trials when their private digital history is exposed without protective boundaries.	Amend the VPA to officially recognize TFGBV survivors as a protected class needing specialized support. Mandate the Victim Protection Board to develop trauma-informed standards, rapid takedown assistance, and safe reporting environments.
Children Act, 2022	Governs child protection, welfare, and safety from exploitation and abuse.	Does not address online peer abuse, cyberbullying, data profiling, or grooming tactics used on modern digital and educational platforms.	Children are exposed to technology-facilitated exploitation on personal and classroom devices without a clear legal framework for protection or recourse.	Introduce specific provisions addressing online child grooming and peer-to-peer cyber-harassment. Mandate strict digital safety safeguards across all educational technology and curriculum deployment platforms.
Counter-Trafficking in Persons Act (CTPA), 2010	Criminalizes human trafficking and coordinates victim identification and support systems.	Lacks explicit recognition of technology-facilitated trafficking, platform-based grooming, or the use of digital financial systems to manage illicit proceeds.	Organized criminal networks operate across borders using social media to recruit and exploit young Kenyan women, frequently escaping trafficking charges due to statutory gaps.	Amend the CTPA to introduce specific provisions on technology-facilitated trafficking. Establish mandatory coordination rules between the Counter-Trafficking Advisory Committee, NC4, and the DCI Cybercrime Unit.

Statute / Instrument	Current Status & Statutory Context	Identified Gaps & Blind spots	Justification & Survivor Implication	Recommended Reforms & Amendments
Employment Act, 2007	Section 6 defines and outlaws' workplace sexual harassment.	Applies primarily to physical workplaces. It fails to explicitly cover digital workspaces, professional messaging apps, or out-of-hours professional digital communications.	Online workplace harassment is frequently dismissed as a personal matter, leading to "Forced Occupational Trauma" where women are driven from their careers.	Amend Section 6 to explicitly define the digital workplace as a full extension of the professional environment. Mandate that employers provide "digital PPE" (security tools, threat monitoring, and legal assistance) for employees facing targeted online abuse.
Media Council Act	Regulates journalist conduct, media standards, and public communications	Does not address coordinated online smear campaigns, algorithmic harassment, or digital safety issues targeting women journalists.	Women journalists face severe online abuse, forcing many to self-censor or leave public-interest reporting entirely.	Integrate gender-responsive digital safety standards into the Media Council Code of Conduct. Establish formal institutional tracking and support systems for journalists targeted by online harassment campaigns.
National Cohesion and Integration Act (NCIA), 2008	Outlaws hate speech, ethnic discrimination, and incitement to violence.	Protects groups based on ethnicity and race but entirely omits gender-based hate speech or targeted misogynistic abuse campaigns.	Coordinated online groups exploit this gap to launch gendered hate campaigns against women in public life, operating with minimal risk of regulatory action.	Amend the NCIA to explicitly include gender as a protected characteristic. Outlaw coordinated gender-based hate speech and targeted digital harassment campaigns designed to silence specific demographics.

Statute / Instrument	Current Status & Statutory Context	Identified Gaps & Blind spots	Justification & Survivor Implication	Recommended Reforms & Amendments
National Gender and Equality Commission (NGEC) Act, 2011	Mandates the Commission to monitor, investigate, and report on gender equality issues.	Lacks an explicit mandate or statutory power to monitor digital spaces, track TFGBV data, or enforce cross-institutional coordination.	The lack of centralized, disaggregated data prevents policy makers from developing targeted, evidence-based legal and fiscal interventions.	Amend the NGEC Act to include digital safety within its core monitoring and investigative mandates. Establish a legal duty for state agencies to share disaggregated data with the Commission
Artificial Intelligence Bill (2026)	Currently before the Senate; introduces a risk-based AI regulatory framework.	It completely omits specific protections for children and lacks provisions addressing gendered AI threats like automated image-stripping applications (“nudify” apps) or model poisoning.	High-risk AI systems are deployed in schools and online spaces without independent oversight, creating risks of child data exploitation and automated gender bias.	Add a dedicated Child Protection Chapter prohibiting commercial profiling of minors and unconsented biometric data collection. Classify image-stripping and deepfake-generating systems as prohibited, high-risk technologies.
NDTCP Regulations 2025 & VASP Act 2025	Regulates digital lenders and virtual asset providers; focuses primarily on financial crime compliance.	Fails to address the use of digital financial platforms or cryptocurrencies to fund cross-border sextortion, tech-abuse campaigns, or identity extortion.	Perpetrators exploit blockchain anonymity to demand extortion payments from survivors, operating with high impunity from traditional financial tracing.	Amend regulations to introduce explicit anti-TFGBV compliance duties. Mandate blockchain transaction tracking and asset forfeiture protocols for addresses linked to digital extortion or sexual coercion.

2.2: REGIONAL AND INTERNATIONAL TREATIES & FRAMEWORKS

International Instrument	Domestic Enforcement Status	Specific Implementation Gaps	Required Alignment Measures
Maputo Protocol (Article 4 & 3)	Ratified by Kenya; legally binding under Article (6)2 of the Constitution.	Lacks explicit application to technology-facilitated violence, leaving digital safety out of formal national compliance monitoring.	Formally integrate digital violence indicators and safety metrics into all statutory state reports submitted under the Maputo Protocol framework.
CEDAW & General Recommendation No. 35	Ratified; establishes clear international legal standards for state accountability.	Domestic victim support networks, including the VPA and Employment Act, do not meet CEDAW's standards for preventing secondary digital victimization.	Update national legal aid programs and judicial training systems to align with CEDAW's standards for comprehensive, cross-border survivor protection.
Budapest Convention on Cybercrime	Accession approved by Kenya.	National evidence laws and mutual legal assistance frameworks lack the fast-tracked cross-border data access systems required by the treaty.	Amend the Evidence Act and CMCA to implement standard 7/24 law enforcement points of contact and streamlined cross-border data sharing.
Malabo Convention (African Union)	Accession approved by Kenya.	The DCI's digital forensics lab and NC4's current statutory powers are under-resourced to meet continental data protection and cybersecurity standards.	Allocate dedicated national budget resources to scale up digital forensic capabilities and align DPA enforcement with continental standards.
ILO Convention 190 (Violence & Harassment)	Currently unratified by Kenya.	National labor laws do not protect employees from technology-facilitated harassment occurring outside standard working hours.	Prioritize the formal ratification of ILO Convention 190 and amend the Employment Act to explicitly cover digital work environment safety.

CHAPTER 3: THEMATIC ANALYSIS OF SYSTEMIC BOTTLE NECKS AND EMERGING RISKS

This chapter presents a comprehensive thematic evaluation of the institutional, technical, and operational challenges that currently hinder effective responses to TFGBV in Kenya. By examining the intersection of systemic enforcement gaps and rapidly evolving digital spaces, this section maps out the critical bottlenecks within the justice pipeline. Furthermore, it analyzes emerging threat vectors, such as advanced synthetic media and algorithmic aggression, to provide a forward-looking framework for protective governance, proactive digital defense, and sustainable policy intervention.

Thematic Category	Current Systemic Status & Evidence	Identified Institutional Bottlenecks	Future Technical Threats & Horizons
Institutional Fragmentation	Survivors are forced to navigate multiple independent agencies (DCI, ODPC, Policare, ODPP, and the Judiciary) without a single point of entry.	There is no integrated case management system or formal cross-agency referral pathway, causing survivors to drop out of the justice process due to exhaustion.	As cross-border cyber-abuse increases, fragmented local systems face growing challenges in tracking complex digital harms across different platforms and jurisdictions.
Enforcement & Evidentiary Deficits	The DCI National Digital Forensic Laboratory faces major backlogs, regularly holding survivor devices for over a year due to a lack of resources.	First responders frequently lack proper training, leading to the mishandling of digital evidence and causing cases to fail standard chain-of-custody rules in court.	The Quantum Computing Threat: Emerging quantum decryption poses a “Harvest Now, Decrypt Later” risk, allowing encrypted survivor data to be targeted for future exposure.

Thematic Category	Current Systemic Status & Evidence	Identified Institutional Bottlenecks	Future Technical Threats & Horizons
Platform Accountability	Global platforms prioritize engagement monetization over local safety, often failing to act on content removal requests within critical early hours.	A major shortage of domestic content moderators fluent in local Kenyan languages and cultural contexts leads to the systemic rejection of valid safety reports.	Algorithmic amplification engines and coordinated bot networks are increasingly weaponized to launch automated, high-velocity smear campaigns.
Child Online Protection	The rollout of the Competency-Based Curriculum (CBC) has introduced AI-driven educational tools into classrooms.	Minors' behavioral, learning, and identity data is collected without clear data governance frameworks or explicit, informed parental consent.	Schoolgirls face immediate risks from AI-driven deepfake generation, online peer grooming, and algorithmic profiling built directly into educational tech.
Intersectional Vulnerabilities	Schoolgirls: Exposure to peer cyberbullying and data exploitation. Women: Targeted by sexual extortion and dating app abuse.	Current legal models use a one-size-fits-all approach that fails to account for the specific needs of rural women, elderly women, and women with disabilities.	The growth of the transnational "manosphere" ecosystem actively funds, organizes, and rewards targeted abuse campaigns against specific demographics.
AI Cybersecurity Threat Vectors	The AI Strategy –2025 2030 remains gender-blind, overlooking how generative AI tools can be weaponized against women.	National cybersecurity frameworks lack mandatory adversarial testing to protect survivor-facing tools and public digital safety infrastructure.	Model Poisoning & Prompt Injection: Malicious actors can corrupt content moderation models or compromise support chatbots to redirect or exploit survivors.

CHAPTER 4: STRATEGIC ACTION ROADMAP AND RECOMMENDATIONS

The nine gaps identified in this policy brief have a common thread i.e. they are all solvable. This chapter sets out specific, time-bound actions organised across three interdependent priority areas, anchored in a gazetted National TFGBV Governance Framework. **The UN Women Model Framework for Legislation on TFGBV (2025)¹**, Kenya's Constitution, and the regional frameworks already ratified by Kenya provide the legal foundation. What is now required is the implementation architecture.

NATIONAL TFGBV GOVERNANCE FRAMEWORK

Gazetted Multi-Sectoral Council: DCI • ODPC • ODPP • NGECC • Civil Society

TRACK A: SURVIVOR-CENTRED JUSTICE

- Standalone TFGBV Protection Act
- Urgent Digital Protection Orders (24hr)
- Comprehensive Civil Restitution Framework
- Integrated survivor support infrastructure

TRACK B: TECHNICAL INFRASTRUCTURE

- Non-invasive data mirroring (DCI Lab)
- Post-quantum cryptographic resilience
- National TFGBV Data Observatory
- Gender-responsive AI regulation

4.1: PRIORITY AREA 1 IMMEDIATE LEGISLATIVE REFORM WITHIN 6 MONTHS

4.1.1. Resolve the CMCA enforcement vacuum: Redraft Sections (1)27(b), (c), and (2)27 of the Computer Misuse and Cybercrimes Act with constitutionally precise language, drawing on the ACHPR Guidelines on Freedom of Expression. The High Court's October 2025 suspension is just a drafting problem with a clear solution, more so as every month without it is another month perpetrators operate freely.

4.1.2 Criminalise AI-generated NCII: Amend the AI Bill 2026 to classify AI systems generating non-consensual intimate imagery as prohibited-risk applications, with criminal liability for both creation and distribution. This will make Kenya the first East African state to explicitly prohibit deepfake sexual abuse.

4.1.3 Enact Urgent Digital Protection Orders: Amend KICA to create statutory Urgent Digital Protection Orders with mandatory 24-hour compliance timelines enforceable against all platforms operating in Kenya. Google rejected %62 of Kenya's content removal requests in H2025 1. Moreover ensuring revenue-calibrated penalties are enacted will make refusals more costly than compliance and thus enhance better compliance.

4.1.4 Add a Child Protection Chapter to the AI Bill 2026: Before the AI Bill is enacted, Parliament must insert provisions prohibiting the commercial profiling of minors, banning unconsented biometric collection, and requiring Child Rights Impact Assessments for any high-risk AI tools deployed in CBC classrooms as these harms are already occurring now, in our Kenyan schools today.

4.2: PRIORITY AREA 2 : INSTITUTIONAL RESTRUCTURING AND CAPACITY BUILDING 6 – 18 MONTHS

4.2.1 Gazette the National TFGBV Coordination Framework: Launch an integrated multi-sectoral framework connecting the DCI, ODPC, Policare, ODPP, and Civil Society under a single case-tracking system with unified survivor intake, mandatory inter-agency coordination, and an annual public accountability report disaggregated by gender, age, disability, and county. Without accountability reporting, coordination remains an aspiration.

4.2.2 Enact a standalone TFGBV Act: A dedicated, gender-responsive Act, informed by the UN Women Model Framework, that defines TFGBV as a distinct category of harm, criminalises deepfakes, voice cloning, sextortion, doxing, and digital coercive control, establishes emergency content removal orders, and mandates a National TFGBV Action Plan with five-year review cycles.

4.2.3 Modernise digital forensic capacity with non-invasive data mirroring: Upgrade the DCI National Digital Forensic Laboratory using non-invasive data mirroring tools so that electronic evidence is preserved to prosecution standards without confiscating survivors' devices for over a year. All forensic investments must meet post-quantum cryptographic standards from inception. What is built without this protection today is a liability against survivors tomorrow.

4.2.4 Strengthen county-level and specialist systems: Fund dedicated technical budgets and specialist training for County Gender Departments. Establish TFGBV-dedicated prosecution units within the ODPP. Gazette NC4's Rapid Reference Guide and Template Charge Sheets for distribution to every police station and prosecutor's office in Kenya. The quality of national TFGBV response is ultimately determined by what also happens for example in Kwale and Bungoma, and not only Nairobi.

4.2.5 Amend the Data Protection Act: Give the ODPC emergency powers to order content removal within hours of a verified TFGBV complaint. Add aggravated harm provisions for TFGBV-related data violations, safety-by-design obligations on platforms, and explicit coordination mechanisms with the criminal justice system. TFGBV must be a named regulatory priority in the ODPC's mandate.

4.3: PRIORITY AREA 3 : SURVIVOR-CENTRED JUSTICE, DATA AND PLATFORM ACCOUNTABILITY WITHIN 18 MONTHS – 3 YEARS

4.3.1 Enforce structural platform accountability: Platforms operating in Kenya with over one million active users must maintain in addition to English, local Swahili (with a view to capture other highly spoken languages including Sheng) moderation capacity, file biannual transparency reports on content removal performance, and subject their recommender algorithms to mandatory gender-disaggregated impact assessments. Google rejected %62 of Kenya's content removal requests in the first half of 2025. That is not a platform failure, rather it is a governance failure, and Kenya has the legislative tools to fix it.

4.3.2 Establish a civil restitution framework: Statutory restitution orders must be made available within criminal proceedings, mirroring the mechanisms already established under the Victim Protection Act 2014 and extended explicitly to TFGBV harm. This means covering documented economic losses, professional setbacks, reputational damage, and the long-term costs of psychological care. A criminal conviction matters, but it does not return a woman's livelihood, her reputation, or the years she lost and thus justice must do more than punish.

4.3.3 Build integrated survivor support infrastructure: Free legal aid in TFGBV cases, safe houses at sub-county level, and TFGBV-specific psychosocial services integrated into existing GBV referral pathways are not optional enhancements to a functioning justice system. They are the precondition for survivors being able to engage that system in the first place. Every woman who cannot afford a lawyer, has nowhere safe to go, or cannot access trauma-informed counselling is a woman for whom every other recommendation in this chapter remains out of reach.

4.3.4 Launch a National TFGBV Data Observatory: Kenya cannot adequately resource or evaluate its TFGBV response without a systematic evidence base. A national data observatory that should be built in partnership with research institutions and civil society, scaling the proof of concept established by the KICTANet OGBV Tracker should track anonymized, disaggregated TFGBV data across gender, age, disability, region, and nature of harm. Without this, policymakers are making decisions in the dark.

4.3.5 Commission a macroeconomic impact assessment: The National Treasury should be directed to quantify the full economic cost of digital silencing i.e. the human capital lost when women are driven offline, the productivity drain on Kenya's knowledge economy, and the fiscal cost of failing to adequately fund survivor services. This assessment exists to make one argument clearly i.e. digital safety is not a social welfare line item in competition with development priorities, rather it is a core economic infrastructure investment, and it should be funded like one.

4.3.6 Ratify and operationalise international commitments: Kenya should ratify ILO Convention 190 on Violence and Harassment and operationalise its accessions to the Budapest and Malabo Conventions through targeted Evidence Act amendments and investment in DCI cross-border investigation capacity.

These instruments are not symbolic rather they unlock the international cooperation Kenya needs to pursue the transnational sextortion networks and cross-border perpetrators that no single country can dismantle working alone.

4.4: HORIZON THREATS: FUTURE-PROOFING THE RESPONSE

4.4.1 AI, deepfakes, and the 2027 electoral cycle: With %149.4 mobile penetration and no current prohibition on AI-generated political content, Kenya's 2027 General Election is extremely vulnerable to AI-enabled electoral TFGBV targeting women candidates. The AI Bill 2026 must prohibit synthetic political impersonation and mandate labelling of AI-generated content in the twelve months before any general election, before the campaign season and not just during it.

4.4.2 Quantum computing and the 'harvest now, decrypt later' threat: Criminal actors are already storing encrypted survivor evidence for future decryption as quantum computing matures commercially. NIST finalised the first post-quantum cryptographic standards in 2024. It follows that all digital forensic and evidence preservation investments must meet those standards from inception. This is because what is built without this protection today is a potential liability against TFGBV survivors tomorrow.

4.4.3 The manosphere and algorithmic amplification: TFGBV has a supply-side infrastructure that criminal law alone cannot dismantle that includes the fact that platforms monetise engagement, and coordinated harassment drives engagement. Mandatory gender-disaggregated algorithmic impact assessments and financial liability for algorithmically amplified TFGBV, embedded in Kenya's platform regulation framework, are the tools to hold platform business models accountable for the harm they are commercially incentivised to amplify.

THREE PRIORITY AREAS. FOURTEEN ACTIONS. ONE COMMITMENT.

Every recommendation in this roadmap is grounded in survivor testimony, aligned with Kenya's constitutional and treaty obligations, and drawn from the practitioners already doing this work albeit with inadequate tools.

The Silicon Savannah will only deliver on its promise if every girl and woman in Kenya in urban centers and rural communities, in a media house and in a rural constituency, in a university and in a primary school or wherever they access the digital realm from, can participate fully, safely, and without fear.

Addressing TFGBV is not a gender equality initiative in competition with Kenya's economic development priorities, rather it is a precondition for those priorities to be realised.

The political will to act is the only variable this roadmap cannot supply.
Everything else is here.

Community Advocacy & Awareness (CRAWN) Trust

4th Floor All African Conference of Churches of Kenya, Waiyaki Way, Westlands.

P.O Box 943-00621, Nairobi, Tel: 020-2664505, E-mail: crawn@crawntrust.org

© **CRAWN Trust**